Department of the Interior
Privacy Impact Assessment

September 10, 2014

Name of Project: Google BlackBerry Enterprise Services
Bureau: Office of the Secretary
Project's Unique ID: 010-000000859

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- Bureau/office IT Security Manager
- Bureau/office Privacy Act Officer
- DOI OCIO IT Portfolio Division
- DOI Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

Also refer to the signature approval page at the end of this document.

A. CONTACT INFORMATION:

Teri Barnett
Departmental Privacy Officer
Office of the Chief Information Officer
U.S. Department of the Interior
1849 C Street, NW, Mail Stop 5547 MIB
Washington, DC 20240
202-208-1605

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) **Does this system contain any information about individuals?**

   a. **Is this information identifiable to the individual[1]?** *(If there is NO information collected, maintained, or used that is identifiable to the*

---

[1] "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

Google BlackBerry Enterprise Services (GBES) is a relay tool that synchronizes data with DOI BlackBerry devices from the Department of the Interior (DOI) BisonConnect Mail, Calendar, and Contacts applications. The BisonConnect Mail, Contacts and Calendar applications do contain personally identifiable information (PII), and the privacy implications have been addressed in the BisonConnect Privacy Impact Assessment. However, GBES does not retain the information synchronized from BisonConnect and does not maintain PII about individuals. GBES uses a Server Relay Protocol (SRP) ID which is a unique number to identify DOI issued BlackBerrys and complete the synchronization of data. GBES stores identifiers of BlackBerry devices such as serial number, model name/type/number, PIN, phone number, WIFI MAC address, MEID/IMEI/SIM information, as part of the device record.

b. **Is the information about individual members of the public?** *(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security documentation).*

GBES is a relay tool that synchronizes data with DOI BlackBerry devices from the DOI BisonConnect Mail, Calendar, and Contacts applications. The BisonConnect Mail, Contacts and Calendar applications contain email correspondence and contact lists that may contain PII about members of the public including contacts lists, senders and recipients of emails, and information contained in email messages. However, GBES only relays this information between BisonConnect and DOI issued BlackBerry devices; GBES does not retain any of the content from BisonConnect, or collect or maintain any PII about individuals. Privacy implications for BisonConnect applications were addressed separately in the BisonConnect Privacy Impact Assessment.

c. **Is the information about employees?** *(If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).*

Yes, the data stored in GBES includes identifiers of BlackBerry devices such as serial number, model name/type/number, PIN, phone number, WIFI MAC address, and MEID/IMEI/SIM, which are part of the BlackBerry device record, and this information may be linked to DOI employees issued BlackBerry devices for official use. Information about employees contained in the BisonConnect Mail, Contacts and Calendar applications, which is synchronized with DOI BlackBerry devices, may

include name, email address, telephone contact information, BlackBerry device telephone number, and other information that may be contained in these applications. However, the GBES system will synchronize this data, and does not collect or retain the data from BisonConnect. Privacy implications for BisonConnect applications were addressed separately in the BisonConnect Privacy Impact Assessment.

2) **What is the purpose of the system/application?**

GBES is a relay tool that synchronizes data with DOI issued BlackBerry devices with the DOI BisonConnect Mail, Calendar, and Contacts applications. The use of GBES enables DOI employees to use DOI issued BlackBerry mobile devices to communicate, view and use the DOI BisonConnect email, calendar and contact applications in the performance of official duties. GBES will be used to establish an account for each DOI BlackBerry user, and each user's email BisonConnect email messages will be pushed to and from the user's BlackBerry device. User's calendar and contacts data will also be replicated as data is updated by users through BisonConnect accounts or BlackBerry devices.

3) **What legal authority authorizes the purchase or development of this system/application?**

Departmental Regulations, 5 U.S.C. 301; The Paperwork Reduction Act, 44 U.S.C. Chapter 35; The Clinger-Cohen Act, 40 U.S.C. 11101, et seq.; OMB Circular A-130, Management of Federal Information Resources; Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service," April 11, 2011; and Presidential Memorandum, "Building a 21st Century Digital Government," May 23, 2012.

C. **DATA in the SYSTEM:**

1) **What categories of individuals are covered in the system?**

GBES synchronizes data for DOI employees, contractors, partners, and volunteers who are issued BlackBerry devices. Data synchronized between BisonConnect and BlackBerry devices contains information about DOI personnel, non-DOI Federal employees, Tribal, State, or local agencies, officials from international or other third party entities, private organizations, and members of the general public. However, though this data passes through GBES during synchronization this data is not retained, maintained, viewable, or retrievable in GBES.

2) **What are the sources of the information in the system?**

a. **Is the source of the information from the individual or is it taken from**

another source? If not directly from the individual, then what other source?

DOI is the primary source of data stored in GBES, which includes serial number, model name/type/number, PIN, phone number, WIFI MAC address, and MEID/IMEI/SIM, which are part of the BlackBerry device record. DOI employees who are issued BlackBerry devices who use BisonConnect email, calendar and contacts applications provide new information and updates as they use these applications and their issued BlackBerry devices. This data is synchronized between BisonConnect and BlackBerry devices, and may contain information from other Federal, Tribal, state, local, territorial, and international agencies, privacy or third-party organizations, and members of the public. However, this data passes through GBES during the synchronization process and is not retained, maintained, viewable, or retrievable in GBES.

b. What Federal agencies are providing data for use in the system?

Contact information, communications and data from other Federal agency employees who communicate with DOI employees are synchronized with DOI BlackBerry devices through GBES. However, this data passes through GBES during the synchronization process and is not retained, maintained, viewable, or retrievable in GBES.

c. What Tribal, state and local agencies are providing data for use in the system?

Contact information, communications and data from Tribal , state, local, territorial, and international agencies who communicate with DOI employees are synchronized with DOI BlackBerry devices through GBES. However, this data passes through GBES during the synchronization process and is not retained, maintained, viewable, or retrievable in GBES.

d. From what other third party sources will data be collected?

Contact information, communications and data from private or third-party organizations who communicate with DOI employees are synchronized with DOI BlackBerry devices through GBES. However, this data passes through GBES during the synchronization process and is not retained, maintained, viewable, or retrievable in GBES.

e. What information will be collected from the employee and the public?

In the course of using the BisonConnect Mail, Contacts and Calendar features as well as their DOI issued BlackBerry devices, DOI personnel may provide personal information that will pass through the GBES system

during synchronization between BisonConnect and BlackBerry devices. The types of personally identifiable information (PII) that users may transmit includes, but is not limited to, name, email address, telephone contact information, BlackBerry device telephone number, and other PII that may be contained in the body, subject, name of attachment, and attachment of email messages, and is limited only by user discretion and compliance with DOI policies concerning PII and proper use of email and electronic resources. However, the GBES system will only hold this data temporarily while synchronization is completed, and will not collect or retain the data. Specific content and communications that passes through GBES during synchronization are not viewable.

As part of its inventory function GBES maintains model name, type and number, PIN, phone number, WIFI MAC address, and MEID/IMEI/SIM information, which are used to identify BlackBerry devices. However, this information is not used as part of the synchronization process between BisonConnect and GBES.

Contact information, communications, calendar updates, data from employees, and communications from members of the public are synchronized with DOI BlackBerry devices through GBES. However, this data passes through GBES during the synchronization process and is not retained, maintained, viewable, or retrievable in GBES. No other information is collected directly from employees or members of the public for use in the GBES.

3) **Accuracy, Timeliness, and Reliability**

a. **How will data collected from sources other than DOI records be verified for accuracy?**

GBES synchronizes data between the BisonConnect system and DOI BlackBerry devices, and does not verify communications or data content for accuracy.

b. **How will data be checked for completeness?**

GBES synchronizes data between the BisonConnect system and DOI BlackBerry devices, and does not verify data content for completeness. GBES only verifies log file indicators that the data synchronization between BisonConnect and BlackBerry devices was completed.

c. **Is the data current?** What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

GBES synchronizes data between the BisonConnect system and DOI BlackBerry devices, which generally occurs in seconds or minutes. GBES log file indicators show the status of data synchronization between BisonConnect and BlackBerry devices. GBES does not otherwise verify the currency of the data content it synchronizes between BisonConnect and DOI BlackBerry devices.

d. **Are the data elements described in detail and documented?** If yes, what is the name of the document?

The data elements are described in detail in the GBES System Security Plan (SSP).

D. ATTRIBUTES OF THE DATA:

1) **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes. GBES is a tool that facilitates DOI employee use of DOI BlackBerry mobile devices by synchronizing data with employees' BisonConnect accounts.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

No, GBES is a tool that facilitates DOI employee use of BlackBerry devices by synchronizing email, calendar and contacts data with the DOI BisonConnect system. GBES does not derive new data or create previously unavailable data about an individual through aggregation from the information collected or communications exchanged. GBES will only hold data temporarily while synchronization is completed, and will not retain information about individuals or the content of data. System administrators will view message headers, log file indications or status on synchronization, and are not able to view specific content that passes through GBES during synchronization.

3) **Will the new data be placed in the individual's record?**

GBES does not retain information about individuals during synchronization, and does not derive new data or create previously unavailable data about an individual through data aggregation.

4) **Can the system make determinations about employees/public that would not be possible without the new data?**

GBES does not collect or retain information about individuals, and does not derive new data or make determinations about individuals.

5) **How will the new data be verified for relevance and accuracy?**

GBES does not collect or retain information about individuals, and does not derive or verify data about individuals.

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Data is not being consolidated. GBES facilitates the use of BlackBerry devices by synchronizing email, calendar and contacts data with the DOI BisonConnect system.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?** Explain.

The BlackBerry devices and the BlackBerry operating systems used by DOI have received Federal Information Processing Standard (FIPS)140-2 certification by the National Institute of Standards and Technology (NIST). FIPS 140-2 is used by the U.S. Federal government to measure mobile device security and validation capabilities and is required under the Federal Information Security Management Act of 2002. GBES will only hold data temporarily while synchronization is completed, and will not retain information about individuals or specific content that passes through GBES during synchronization. Only log file indications or status on synchronization are available to system administrators. GBES logs maintain the username and message IDs in order to identify and verify synchronization.

8) **How will the data be retrieved? Does a personal identifier retrieve the data?** If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data about individuals is not retrieved in GBES. GBES is a tool used to synchronize data between the DOI BisonConnect system and DOI BlackBerry, devices, and does not retain information about individuals. The GBES system will only hold the data temporarily while synchronization is completed.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

GBES allows system administrators to run reports on DOI BlackBerry devices, to include information regarding carrier and mobile phone number, model number, serial number, and reports on number and types of BlackBerry

devices used for annual servicing.

The GBES auditing system allows reports to be generated on various aspects of the system's operating controls, including system functions and user actions; however, these reports provide only aggregated information and not information specific to individuals.

10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

Generally, users do not have the opportunity to decline to provide the information synchronized between BisonConnect and GBES as that information comes from the BisonConnect system. However, individuals may limit the information that they enter into their BlackBerry devices or provide in BisonConnect by exercising discretion with respect to the PII they provide in BisonConnect, including limiting PII in their contacts, calendars, and emails.

E. <u>**MAINTENANCE AND ADMINISTRATIVE CONTROLS:**</u>

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The system servers are hosted, managed, and administered in a cloud hosted environment by Exchange My Mail (EMM). EMM is required to provide and meet the Federal Information Security Management Act (FISMA) security requirements as established in the Federal Acquisition Regulation (FAR).

2) **What are the retention periods of data in this system?**

Records generated by GBES are maintained in accordance with Office of the Secretary records series 1400, General System Records, approved by the National Archives and Records Administration (NARA). Records disposition is generally temporary and retention periods vary dependent on the type of record created.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Records are disposed of in accordance with approved records disposition methods. Paper records are shredded, and electronic records are degaussed or erased in accordance with the 384 Departmental Manual 1 and NARA guidelines.

4) **Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No, the system is not using technologies in ways that DOI has not previously employed. DOI has used BlackBerry mobile devices and associated integration services for many years.

5) **How does the use of this technology affect public/employee privacy?**

Although mobile devices may present some unique and enhanced security and privacy concerns, DOI issued BlackBerry devices are secured in a manner that should make any such risk negligible. The BlackBerry devices and the BlackBerry operating systems used by DOI have received FIPS140-2 certification by NIST. FIPS 140-2 is used by the U.S. Federal government to measure mobile device security and validation capabilities and is required under the FISMA.

The GBES does not maintain PII on individuals so there is no risk of unauthorized access, use, or disclosure of individual PII in the system. There is a minimal privacy risk for the data that is synchronized through the GBES. However, the risk is mitigated by a variety of controls including encryption, security audit features, passwords, Rules of Behavior, and mandatory security, privacy and records management training.

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

GBES does not monitor individual users. GBES does provide an auditing feature, which is maintained by EMM. Audit logs can be used to aggregate user activity; however, specific details of this activity are not available.

7) **What kinds of information are collected as a function of the monitoring of individuals?**

Not applicable. GBES does not monitor individual users. The GBES auditing system allows reports to be generated on various aspects of the system's operating controls, including system functions and user actions; however, these reports provide only aggregated information and not information specific to individuals.

8) **What controls will be used to prevent unauthorized monitoring?**

Access to audit logs will be granted to system administrators on a limited basis, and only authorized administrators who have been given a username and password will be able to access the system. In addition, all users must

sign the DOI Rules of Behavior and complete Federal Information System Security Awareness (FISSA), Privacy and Records Management training before being granted access to any DOI IT resource, and annually thereafter.

9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

GBES does not maintain PII on individuals and is not a Privacy Act system of records.

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

GBES does not maintain PII on individuals and is not a Privacy Act system of records.

F. ACCESS TO DATA:

1) **Who will have access to the data in the system?** (E.g., contractors, users, managers, system administrators, developers, tribes, other)

System Administrators, including contractors, will be granted access to GBES system data and system audit logs in order to provide support and to monitor proper system use, including performing system usage audits. Access procedures are described in the GBES system assessment and authorization (A&A) documentation and the system security plan.

2) **How is access to the data by a user determined?** Are criteria, procedures, controls, and responsibilities regarding access documented?

System Administrators, including contractors, will be granted access rights on a least privileges basis, which will permit minimal access needed in order to perform necessary job functions. Access procedures are described in the GBES system A&A documentation and the system security plan.

3) **Will users have access to all data in the system or will the user's access be restricted? Explain.**

End users will have no access to information contained within GBES, (i.e, Audit log, configurations, etc.) Only System Administrators and authorized personnel will have access to system data and audit logs, in order to provide support and monitor proper system usage.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

GBES does not maintain PII on individuals. Access will be granted based on least privileges and access required to perform necessary job functions. GBES system audit log can be used to run reports on authorized users' access to and actions within GBES, such as date and time of day a user accessed the system and any changes to account privileges. Access to audit logs will be granted to system administrators and security personnel on a limited basis, and only authorized administrators who have been given a username and password will be able to access the system. In addition, all users must sign DOI Rules of Behavior and complete FISSA, Privacy and Records Management training before being granted access to any DOI IT resource, and annually thereafter.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

   Yes, contractors were involved with the design and development of the system and will be involved with the maintenance and operation of the system. Federal Acquisition Regulation (FAR) contract Clause 52.224-1, Privacy Act Notification (April 1984), Federal Acquisition Regulation (FAR) contract Clause 52.224-2, Privacy Act (April 1984), Federal Acquisition Regulation (FAR) contract Clause 52.239-1, Privacy or Security Safeguards (Aug 1996) and 5 U.S.C. 552a are included by reference in the agreement with the contractor.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

   As discussed above, most data that flows through GBES will be obtained from BisonConnect Mail, Contacts and Calendar features. Email and calendar and contact information created in GBES will be integrated into BisonConnect. BisonConnect is the only system that shares or receives data from GBES.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   The System Owner and System Administrators will be responsible for protecting the privacy rights of the public and employees affected by the interface.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

   No other agency will have direct access to or share data from the GBES system.

9) How will the data be used by the other agency?

No other agency will have direct access to or share data from the GBES system.

10) Who is responsible for assuring proper use of the data?

The System Owner and System Administrators for GBES will have the ultimate responsibility for protecting the privacy rights of the public and employees affected by the system.